International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 2 Issue: 11 3494 – 3498

Detailed Concept of Network Security

Er. Anup Lal Yadav
M-Tech Student

Er. Sahil Verma
Asst. Prof. in C.S.E. Deptt.
EMGOI , Badhauli.
sahilkv4010@yahoo.co.in

Er. Kavita
Asst. Prof. in C.S.E. Deptt.
EMGOI , Badhauli.

Abstract:-Computer world security management is essential resource for all the latest news, analysis, case studies and reviews on authentication, business continuity and disaster recovery, data control, security infrastructure, intellectual property, privacy standards, law, threats cyber crime and hacking and identity fraud and theft. This section covers secrecy, reliable storage and encryption. security, protecting data from unauthorized access, protecting data from damage and ROM either an external or an internal source, and a disgruntled employee could easily do much harm.

Key Area:- *Secrecy, Non-repudiation, cryptography, security, reliable storage and sub topics.*

*****

INTRODUCTION

Computers networks were primarily used by university researchers for sending email, and by corporate employers for sharing printers. These security terms did not get a lot of attention. But now as millions of ordinary citizens are using networks for banking, shopping and filling their tax returns. Network security is one of the major problem in computer world or we can say that in technology field. Network Security problems can be divided roughly into four interwined area. Secrecy, authentication, nonrepudiation and integrity control.

1. Secrecy: It has to do with keeping information out of the hands of unauthorized users. When people think about network security what is usually comes to mind.
2. Authentication: It deals with determining whom you are talking to before revealing sensitive information as entering into a business deal.
3. Non Repudiation: It deals with signatures.

Secrecy and Integrity are achieved by using registered mail and locking documents up.

SECURITY

Network Security, protecting data from unauthorized access, protecting data from damage and development and implementing policies and procedures for recovery from breaches and data losses. It is worth spending a few moments considering where in the protocol stack network security belongs. There is probably no one single place. Every layer has something to contribute. In the physical layer wiretapping can be failed by enclosing transmission lines in sealed tubes containing argon gas at high pressure. Any attempt to drill into a tube will release same gas, reducing the pressure and triggering an alarm. [3]

Some military systems use this technique. The data link layer packets on a point-to-point line can be enclosed as they leave one machine and decoded as they enter another. This solution breaks down when packets have to traverse multiple routers, however because packets have to be decrypted at each router leaving them vulnerable to attacks from within the router. Nevertheless, link encryption as this method is called encrypted data. The transport layer entire connections can be encrypted, end to end, that is process to process. Although these solutions helps with secrecy issues and many people are working hard to improve them, none of them solve authentication or non repudiation problem in a sufficiently general way. The network layer firewalls can be installed to keep packets in or keep packets out.

FIREWALLS

A firewall is a device (usually a router or a computer) installed between the internal network of an organization and the rest of the internet. It is designed to forward some packets and filter others. A firewall is usually followed by a packet filter firewall or a proxy based firewall.

Any network that is connected to the internet should pass communication through a firewall. A firewall is a combination of hardware and software that prevents unauthorized access to an internal network from outside. All messages entering or leaving a network pass through the firewall which examines each message and blocks those that do not meet the specified security criteria. A firewall filters out traffic that should not pass between the internet and your private network, such as messages between two computers within your private network.

Packet- filter Firewall

A firewall can be used as a packet filter. It can forward or block packets based on the information in the network layer and transport layer headers. Source and destination IP address source and destination port addresses and type of protocol (TCP or UDP). A packet filter firewall is a router that uses a filtering table to decide which packets must be discarded.

HOW DOES A FIREWALL WORK ?

A firewall prevents direct communication between network and external computers by routing communication through a proxy server located outside of the network. The firewall determines if it is a safe to let a file pass to the network and from the network. A firewall is also called a security-edge gateway.

MICROSOFT PROXY SERVER

Microsoft provides software that combines the features of a proxy server and firewall into a single product Microsoft proxy server.

HOW DOES MICROSOFT PROXY SERVER WORK ?

Microsoft Proxy Server acts as a secure gateway between your LAN and the Internet. A gateway enables two different networks to communicate. Proxy Server provides a connection to the internet for your group, division, or your entire intranet. Proxy server also acts as a secure gateway and a firewall by allowing inbound access from the internet to your network.

By using a Proxy server gateway you can secure your network against intrusion. Proxy Server enables you to make requests to the internet and to receive information, but it prevents unauthorized users from accessing your network. You can configure proxy server to enable your workstations to communicate with remote services on the internet. For implementing we have adequate bandwidth for the internet connection and choose the level of security at which you want to protect you LAN.

Reliable Storage

The most common RAID configurations. However, there are other, more obscure types available to as well. To learn more about the RAID arrays I talk about below.

RAID 0

A RAID 0 array is what's known as a stripe set with no fault tolerance. The basic idea is that multiple physical hard drives are treated as a single volume. Rather than only combining the storage capacity of those drives though, a RAID 0 array also combines the performance of each drive by simultaneously writing to each one.

For example, suppose that you needed to write a file to a RAID 0 array consisting of three hard drives (the minimum requirement for a RAID 0 array is two drives). The file would basically be broken into three pieces, with a third of the file being written to each drive. Since the write operations occur simultaneously, the file is written to disk roughly three times faster than it could be written to a comparable single disk.

The advantages of a RAID 0 array are its speed and that the full capacity of each drive in the array is available for storage. The disadvantage is that RAID 0 offers no fault tolerance. If a drive within the array fails, the entire volume is destroyed and all data is lost.

RAID 1

RAID 1 involves a technology known as mirroring (sometimes called disk duplexing). The idea behind RAID 1 is that any data written to one drive is also written to another. If a drive fails, you've got a copy of your data already stored on another drive.

There are a couple of disadvantages to RAID 1 though:

- The first disadvantage is speed. When it comes to writing data, RAID 1 is no faster than a comparable single disk. Although, some RAID 1 implementations allow you to read data at double the speed of a comparable single disk by reading half of the data from each drive in a simultaneous read operation.
- The other disadvantage to RAID 1 is overhead. You've got an entire hard drive that is being used as a spare. Therefore, it can't be used for data storage in the traditional sense.

RAID 0+1

RAID 0+1 is basically a mirrored RAID 0 array. RAID 0+1 provides the same level of fault tolerance as RAID 5, and the same overhead for fault tolerance as RAID 1. In plain English, this means that if a drive in your RAID 0+1 setup fails, the array continues to function.

However, because you're mirroring an entire array, there is a lot of overhead. For example, if your RAID 0+1 array consists of 10 hard disks, you are only going to be able to use five of those disks for storing data. The other five act as a mirror.

The minimum requirement for setting up a RAID 0+1 array is four drives (a mirrored set of a two drive stripe set).

RAID 5

UA RAID 5 array is very similar to a RAID 0 array, but with one major difference: fault tolerance. RAID 5 arrays are usually referred to as stripe sets with parity. What this means is that a RAID 5 array is a stripe set just like a RAID 0 array. But unlike a RAID 0 array, if a disk within the array fails, the volume will not be corrupted. In fact, the volume

 ISSN: 2321-8169
3494 – 3498

can continue to function while the system is waiting for you to replace the failed disk.

So what's the catch? The fault tolerant abilities of RAID 5 come at a cost of one of the drives in your array. For example, if your array consists of five hard drives (three is the minimum), then you will only have access to the capacity of four of those drives. That's because a portion of each drive stores parity information used to keep the array going should a drive fail.

When the failed disk is eventually replaced, this parity information is used to replace the data that previously existed on the failed disk. Regardless of the size of your RAID 5 array, the parity information consumes the equivalent of one disk worth of data.

Writing parity information and data to each drive also has an effect on throughput. A RAID 5 array is not as fast as a comparable RAID 0 array -- but the decrease in speed is often worth it given the array's fault tolerant nature.

Cryptography

Public-key cryptography, also known as **asymmetric cryptography**, is a form of cryptography in which the key used to encrypt a message differs from the key used to decrypt it. In public key cryptography, a user has a pair of cryptographic keys—a **public key** and a **private key**. The private key is kept secret, while the public key may be widely distributed. Incoming messages would have been encrypted with the recipient's public key and can only be decrypted with his corresponding private key. The keys are related mathematically, but the private key cannot be practically derived from the public key.

As the world increasingly turns to electronic business, electronic credentials that prove identity are becoming a critical necessity. Much like a passport proves identity in the offline world, public-key infrastructure (PKI) delivers a way to prove identity in the online world.

PKI is fast becoming the cornerstone of information security technology for a large number of companies.

PKI ensures that people are who they say they are and also proves that documents haven't been tampered with, which is critical when conducting online transactions, such as placing orders or transferring money. Here's a simplified look at these state-of-the-art passports to the online world.

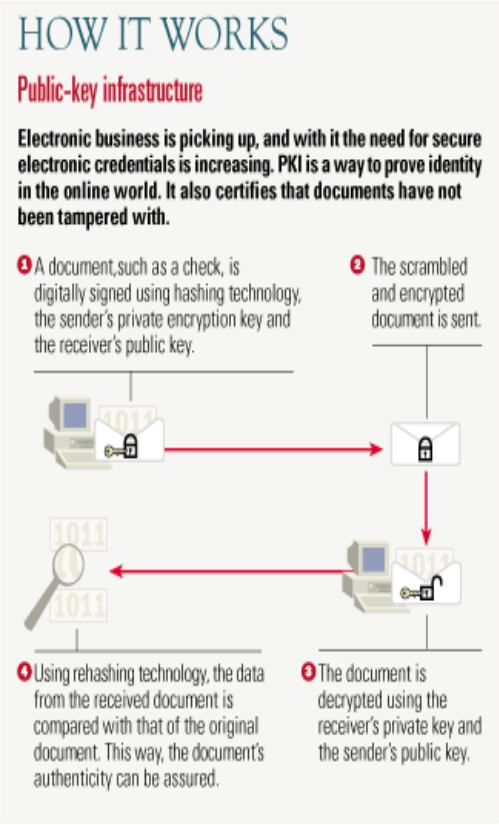
The two main branches of public key cryptography are:

- Public key encryption — a message encrypted with a recipient's public key cannot be decrypted by anyone except the recipient possessing the corresponding private key. This is used to ensure confidentiality.
- Digital signatures — a message signed with a sender's private key can be verified by anyone who has access to the sender's public key, thereby proving that the sender signed it and that the message has not been tampered with. This is used to ensure authenticity.

Public-key cryptography comes in. A large piece of data set to be encoded - for instance, a document - is run through a complicated mathematical computation to generate a single large number, called a hash. The original data and the hash are inextricably linked. If either changes, the hash won't match and the message cannot be decoded.

To digitally sign a document, a hash is taken of the document and then signed with a user's (let's call him Bob) private key. Data scrambled with Bob's private key can only be unscrambled with Bob's public key. Any entity can verify the validity of the document by unscrambling the hash with Bob's public key and checking that against another hash computed from the received data.

If the hashes match, the data was not tampered with and Bob's digital signature is on it. But because I didn't watch Bob sign the document, I don't know that it wasn't signed by an imposter. This issue is solved because only Bob has his private key, and so he is the only one who could have signed the document.



Disadvantage

Major weaknesses have been found for several formerly promising asymmetric key algorithms. The 'knapsack packing' algorithm was found to be insecure when a new attack was found. Recently, some attacks based on careful measurements of the exact amount of time it takes known

hardware to encrypt plain text have been used to simplify the search for likely decryption keys. Thus, mere use of asymmetric key algorithms does not ensure security; it is an area of active research to discover and protect against new attacks.

Potential security vulnerability in using asymmetric keys is the possibility of a man in the middle attack, in which communication of public keys is intercepted by a third party and modified to provide different public keys instead. Encrypted messages and responses must also be intercepted, decrypted and re-encrypted by the attacker using the correct public keys for different communication segments in all instances to avoid suspicion. This attack may seem to be difficult to implement in practice, but it's not impossible when using insecure media (e.g. public networks such as the Internet or wireless communications). A malicious staff member at Alice or Bob's ISP might find it outright easy.

Protection through Encryption

Some encryption schemes can be proven secure based on the presumed hardness of a mathematical problem like factoring the product of two large primes or computing discrete logarithms. Note that "secure" here has a precise mathematical meaning, and there are multiple different (meaningful) definitions of what it means for an encryption scheme to be secure. The "right" definition depends on the context in which the scheme will be deployed.

In contrast to the one-time pad, no public-key encryption scheme can be secure against eavesdroppers with unlimited computational power. Proofs of security therefore hold with respect to computationally-limited adversaries, and give guarantees (relative to a particular mathematical assumption) of the form "the scheme cannot be broken using a desktop computer in 1000 years".

The most obvious application of a public key encryption system is confidentiality; a message which a sender encrypts using the recipient's public key can only be decrypted by the recipient's paired private key.

Public-key digital signature algorithms can be used for sender authentication and non-repudiation. For instance, a user can encrypt a message with his own private key and send it. If another user can successfully decrypt it using the corresponding public key, this provides assurance that the first user (and no other) sent it. In practice, a cryptographic hash value of the message is calculated, encrypted with the private key and sent along with the message (resulting in a cryptographic signature of the message). The receiver can then verify message integrity and origin by calculating the hash value of the received message and comparing it against the decoded signature (the original hash). If the hash from the sender and the hash on the receiver side do not match, then the received message is not identical to the message which the sender "signed", or the sender's identity is wrong.

To achieve authentication, non-repudiation, *and* confidentiality, the sender would first encrypt the message using his private key, then a second encryption is performed using the recipient's public key.

Conclusion

To provide network reliability, it is also important to do preplanning and /or advanced preparation. However there can be a failure in the network that can actually take away the capacity . The security of these computers thus is essential. A fair amount of research effort has been developed over the past decades to the general topic of computer security, and the results of this research are applicable to the computer aspect of network security.

Security Management

Security management is responsible for controlling access to the network based on the predefined policy. This separation results in increased network security, reliability, and efficiency while also giving a higher level of service to network users long with new "intelligent" services. Transmission routes are often duplicated to offer security in terms of alternate routing in time of emergency.

Cryptography

Public-key cryptography is not necessary and secret-key cryptography alone is sufficient. This includes environments where secure secret-key agreement can take place, for example by users meeting in private. It also includes environments where a single authority knows and manages all the keys, e.g., a closed banking system. Since the authority knows everyone's keys already, there is not much advantage for some to be "public" and others "private." Also, public-key cryptography is usually not necessary in a single-user environment. For example, if you want to keep your personal files encrypted, you can do so with any secret-key encryption algorithm using, say, your personal password as the secret key. In general, public-key cryptography is best suited for an open multi-user environment.

REREFRENCE

[1] M. Steinder and A.S. Sethi, ``Multi-Domain Diagnosis of End-to-End Service Failures in Hierarchically Routed Networks." In NETWORKING 2004, Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications (N. Mitrou, K. Kontovasilis, G.N. Rouskas, et al. (eds.)) Lecture Notes in Computer Science Vol. LNCS-3042, (2004),

[2] TExpert system based automatic network fault management system
C. Sheng,H.-D. Hung,. Dept. Of Electr. & Computer Eng., Texas Univ., Austin, TX;

[3] ANDREW S. TANENBAUM Computer Networks, Vrije University Amsterdam, The Netherlands, 2003

[4] Behrouz A.Farouzan, DeAnza College, 2006

[5] KARPAGAM JCS, Journal of Computer Science, Mar-Apr 2008 Volume-2, Issue 3
[6] Deepankar Medhi Article University of Missouri-Kansarcity Network Reliability and fault tolerance
[7] Byte Sphere article, http://www.oldview.com/network_fault_management.html
[8] William Stallings, DATA AND COMPUTER COUMMNICATIONS,'Sixth Edition.
[9] ED TITTEL, Theory and Problems of Computer Network.SCHAUM'sOutline, Austin Community. College.